SHARP

SECURITY SOLUTION
セキュリティソリューション

シャープ デジタル複合機

セキュリティガイド

デジタル複合機を安心してお使いいただくために

もくじ

1 はじめに 3
2 複合機のセキュリティに対するシャープの取り組み.....4
3 複合機のセキュリティ 6
デジタル複合機のセキュリティとは .....
セキュリティの脅威と脅かされる情報資産.....
4 セキュリティの脅威と求められる セキュリティソリューション 7
外部からの不正アクセスによる情報漏洩 8
デジタル複合機内データからの情報漏洩 10
ネットワーク入出力データへの不正アクセスによる 情報漏洩 14
誤送信による情報漏洩 15
出力した紙文書の持ち去りによる文書データの漏洩 16
不正コピーによる文書データの漏洩 16
権限の無いユーザーの使用による可用性の低下や データの漏洩..... 17
使用状況の把握、および情報漏洩の心理的な抑止対策 18
5 機種別搭載セキュリティ機能一覧表.....19
問い合わせ先..... 23

1 はじめに

平素は、シャープのデジタル複合機をご愛用頂き、誠にありがとうございます。
シャープのドキュメントセキュリティシステムは、デジタル複合機を利用するお客様の大切なデータを守るため、想定されるさまざまな脅威への対策を用意しております。
本書をご一読いただき、適切な環境を構築し、適切な対応を選択頂くよう、お願いいたします。

2 複合機のセキュリティに対するシャープの取り組み

シャープは、デジタル複合機のデータセキュリティにいち早く取り組み、2000 年 4 月、米国をはじめ海外向けにデータセキュリティキットを発売。2001 年 4 月には、米国認証機関から複写機・プリンター業界では世界で初めて「Common Criteria EAL2」の認証（セキュリティ認証）を取得しました。2002 年 12 月には、日本を含む全世界向けデータセキュリティキット AR-FR4 が「Common Criteria EAL2」のセキュリティ認証を取得。更に 2004 年 9 月には一般商用製品として現状最高レベルと言える「Common Criteria EAL4」認証を業界で初めて取得しました。

この EAL4 という評価保証レベルは、ソースコードレベルによるセキュリティ機能の確認と、開発体制や管理体制といった品質システムまで幅広く厳密に評価された結果、シャープのこれらの製品が、開発からお客様の手に渡るまで、第三者により改ざんされることなく、間違いなく機能することが保証されているということを表しています。

コモンクライテリアとは

コモンクライテリア（Common Criteria）とは、情報システムやそれを構成するハードウェア／ソフトウェアの IT 製品について、目標となるセキュリティ保証レベルを基準に基づいて評価するための国際規格の名称です。
1999 年 12 月に「ISO/IEC15408 情報技術セキュリティ評価基準」として国際規格化されました。
1998 年 10 月、米英独仏加の 5ヵ国により CCRA（Common Criteria Recognition Arrangement）が設立され、Common Criteria に基づき評価・認証された IT 製品は、認証を取得した国だけではなく、CCRA に加盟している他国でも認証の適用が認められます。日本では、2000 年 7 月に ISO/IEC15408 が「JIS X 5070」として JIS 化、2001 年 4 月に、「IT セキュリティ評価及び認証制度（JISEC）」が創設され、2003 年 10 月に CCRA に加盟しました。

EAL（評価保証レベル）とは

EAL は、Evaluation Assurance Level の略で、評価の厳格さのレベルです。EAL の上位レベルは、下位レベルで定義されている評価内容を含んでいます。
EAL はセキュリティ機能の強度を表すものではなく、あくまで評価内容の厳格さを示すものです。したがって、EAL のレベルと評価対象のセキュリティ機能強度は一致しません。
たとえば、シャープのデータセキュリティキット「AR-FR1/FR2/FR3」は、Common Criteria EAL2 の認証を取得していますが、セキュリティ機能の強度は、EAL の上位レベルに劣るものではありません。
EAL は、下表の 7 段階で定義されています。

レベル	概要	主な用途
EAL7	形式的な設計の検証と評価	政府機関・軍事用途向け
EAL6	半形式的な設定の検証と評価	政府機関・軍事用途向け
EAL5	半形式的な設定と評価	政府機関・軍事用途向け
EAL4	体系的な設計と評価及びレビュー	民生・政府機関・軍事用途向け
EAL3	体系的な評価と確認	民生用途向け
EAL2	構造的な評価	民生用途向け
EAL1	機能的な評価	民生用途向け

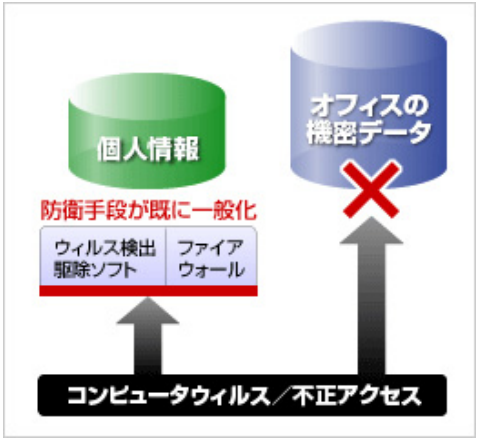
※ データセキュリティキットのコモンクライテリア認証取得状況は、巻末の機種別搭載セキュリティ機能一覧表をご参照ください。

シャープはデジタル複合機の企画開発段階から、お客様のオフィス環境におけるセキュリティの脅威を想定し、あらゆる知識と技術を結集してその対策を提供しております。
また、進化し続けるネットワーク技術により変化するお客様のオフィス環境では、デジタル複合機に対するセキュリティの脅威も日々進化しています。この過程で、デジタル複合機のシステムに対する脆弱性が発見された場合には、速やかに対応を行っております。

3 複合機のセキュリティ

デジタル複合機のセキュリティとは

ネットワーク環境の急速な発展とコンピューターの普及に伴い、コンピューターウィルスや外部からの不正アクセス、機密データ漏洩等の情報犯罪が急増し、深刻化しています。
このような状況下で自らを守るためには、リスクに対して効果的な防衛手段が必要なのは言うまでもありません。コンピューターウィルスに対してはウィルス検出 / 駆除ソフト、不正アクセスに対してはファイアウォールというように、従来から危険視されていた情報犯罪については有効な防衛手段が既に一般化しています。しかしながら、オフィスの情報漏洩という問題に対しては、いまだ利用者のモラルに依存しているというケースが多いのではないでしょうか。



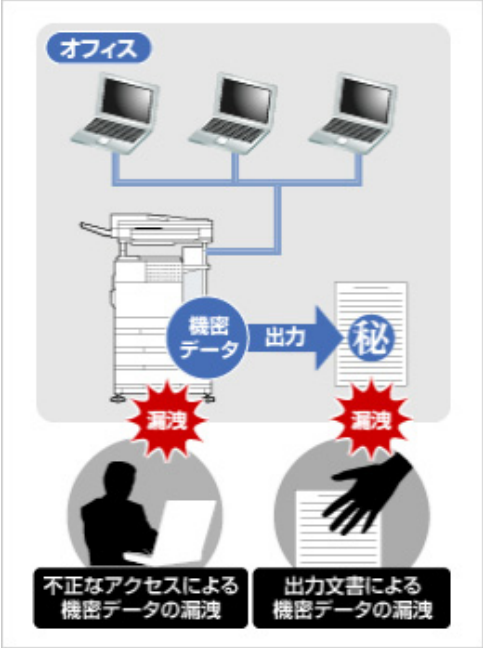
2005 年 4 月に全面施行された「個人情報保護法」をはじめとした、法令の整備などに伴って内部統制・コンプライアンスの重要性が増す中、今やあらゆるオフィスにおいて情報セキュリティはなくてはならないものになってきていると言えます。

セキュリティの脅威と脅かされる情報資産

オフィスでは毎日、重要な情報が扱われています。顧客データや未発表の新商品情報、経営 / 人事情報. . . 。

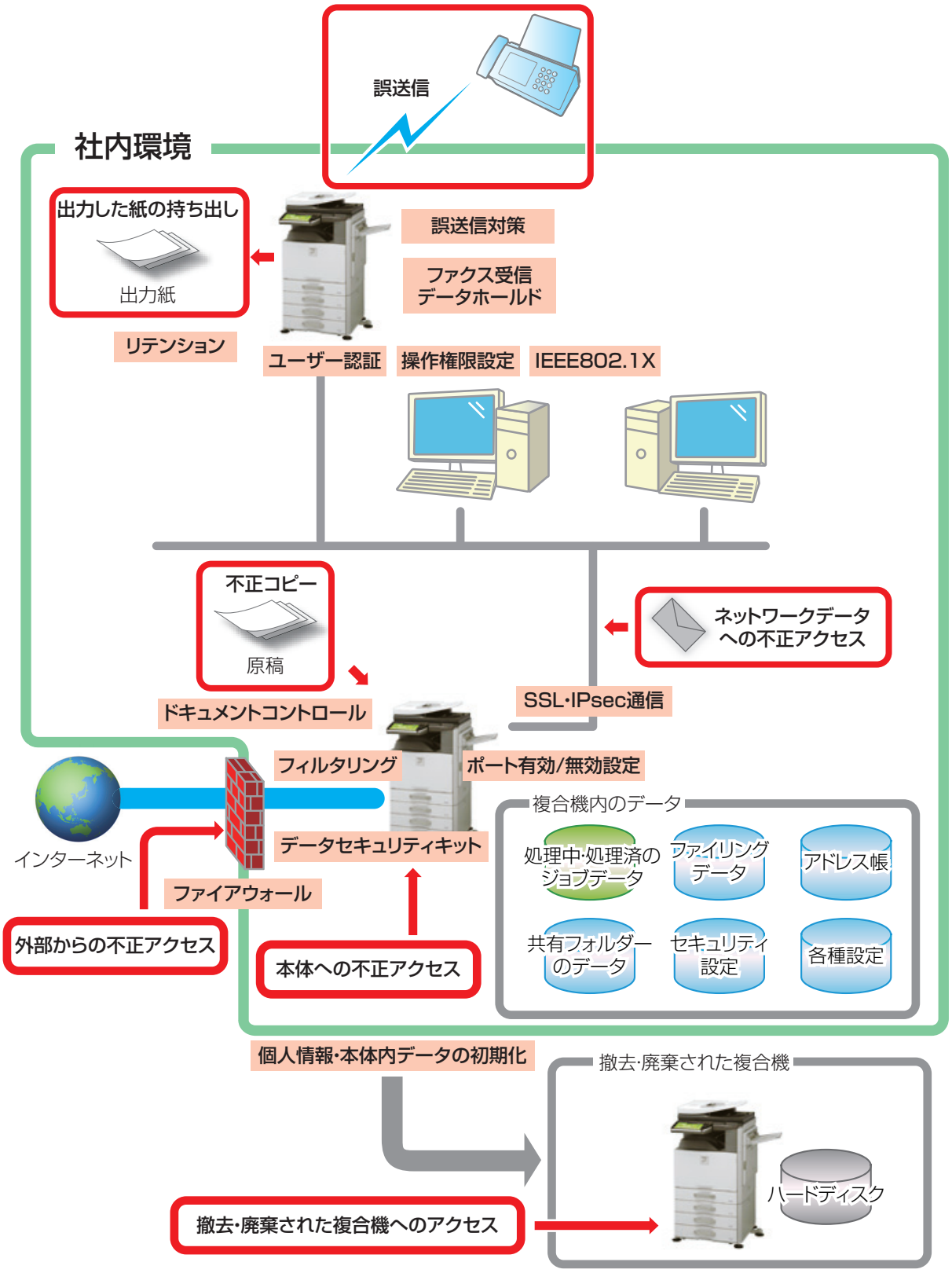
もし万が一、これらの重要な情報が、悪意を持つ者に閲覧・利用された場合、どうなるでしょうか？お客様や取引先からの信用は失われ、経営に深刻なダメージを受けることはもちろん、情報の種類によっては、企業としての社会的責任を問われることもあるでしょう。企業や組織にとって、機密情報の漏洩は致命的です。

このように機密情報が漏洩することによりもたらされる被害の深刻さは容易に想像できると思いますが、その反面、日常の業務においてその危険性を認識している方は少ないのではないでしょうか。しかし、オフィスで扱われるデータは、漏洩の危険と常に隣り合わせなのです。



4 セキュリティの脅威と求められるセキュリティソリューション

お客様のオフィス環境や取り扱う情報に対して、どのような脅威が考えられるでしょうか。
それらの脅威に対して、シャープがご提供するソリューションについてご説明いたします。



外部からの不正アクセスによる情報漏洩

● 脅威

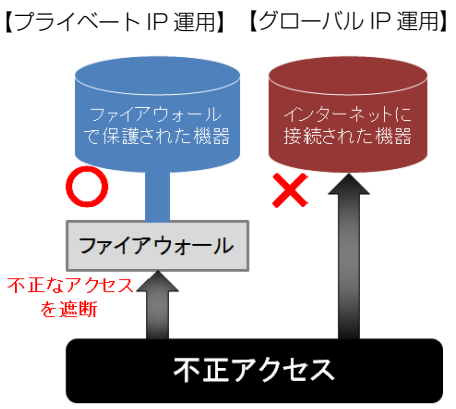
ファイアウォール等、外部からのアクセスを防御する機器を設置せずインターネットへ接続している場合は、インターネットからの攻撃に直接さらされる危険性があります。具体的には、複合機 Web ページにブラウザーから直接アクセスされ、セキュリティ設定や受信データの転送先情報を変更されたり、以下のようなデータを不正に閲覧、取得されたりする可能性があります。

- デジタル複合機に保存したドキュメントファイリングデータ
  - ▶ 一時保存フォルダー内のデータ
  - ▶ 標準フォルダー内のパスワードの設定されていないデータ
  - ▶ パスワードの設定されていないユーザーフォルダー内のパスワードの設定されていないデータ
- アドレス帳のエントリー (名前、メールアドレス、ファクス番号等)
- 共有フォルダーのデータ

● 対策

基本的には、IPv4 環境ではプライベート IP アドレスでの運用をお願いします。

ネットワークに接続されるデジタル複合機は、ファイアウォールや UTM(統合脅威管理) 機器、ブロードバンドルーター等、外部からの接続を制御する機器を介して接続して頂くことにより、外部からの不正なアクセスを遮断することができます。



一般的なオフィス環境においては、利用可能な IPv4 アドレスが逼迫していることからルーター機器をお使い頂いている場合がほとんどであり、プライベート IP アドレス (インターネットから分離され、オフィス内のみに利用を制限した IP アドレス) での運用となりますので、外部からのアクセスを遮断することができます。しかしながら、一部環境においては、グローバル IP アドレス (直接インターネットに接続する際に使用される IP アドレス) にて接続されている場合があり、外部からの不正なアクセスが行われる危険性があります。速やかにプライベート IP アドレスへ変更頂くことで対応が可能となります。

お客様のネットワーク環境がファイアウォール等により外部からのアクセスから保護されているかどうかをご判別いただくには、デジタル複合機にプライベート IP アドレスが割り当てられていることをご確認ください。

プライベート IP アドレスは、以下の範囲と定義されています。

プライベート IP アドレスの範囲		
10.0.0.0	～	10.255.255.255
172.16.0.0	～	172.31.255.255
192.168.0.0	～	192.168.255.255

※ デジタル複合機に割り当てられている IP アドレスの確認方法については、お買い上げの販売店にお尋ねください。

管理者パスワードを工場出荷時の初期値から変更して下さい。
複合機 Web ページを操作するためには、所定のパスワードを入力（管理者としてログイン）する必要があります。
デジタル複合機の工場出荷時には、管理者パスワードが設定されていますが、パスワードの初期設定値は取扱説明書にも記載されており、誰でも容易に知ることができます。管理者が変更するとともに、厳重に管理して下さい。

※ 管理者パスワードの変更方法については、お買い上げの販売店にお尋ねください。

デジタル複合機内データからの情報漏洩

デジタル複合機は、電子ソートなど、その多彩な機能を実現するために、一旦ハードディスクなどのメモリ装置にコピー / プリント / ファクス / ネットワークスキャンなどのジョブデータを一時的に保存する仕組みになっています。また、デジタル複合機によっては、これらのジョブデータを後で再利用するためにファイリング機能を有しているものもあります。

本体メモリ装置の持ち出しによる情報漏洩

● 脅威

ジョブデータやファイリングデータを保存したデジタル複合機内のハードディスクやフラッシュメモリー等のメモリ装置を不正に持ち出すことにより、情報漏洩する可能性があります。

● 対策

データセキュリティキット

シャープのデータセキュリティキットは、暗号化、実データ消去、パスワード保護機能により高い安全性を確保しています。

※ 製品によっては、一部の機能に対応しない場合があります。

機能

■暗号化

ジョブデータとドキュメントファイリングデータは、デジタル複合機内の記憶装置に保存されています。これらのデータを暗号化することにより、たとえ何らかの方法でデータを入手できたとしても、復元できない状態となります。

■実データ消去

通常、ジョブデータやドキュメントファイリングデータは、消去操作を行っても実データ部は消去されません。これは、ジョブデータやドキュメントファイリングデータの所在を示す情報だけを消去しているためです。したがって、一見、消去されたように見えていても、実際には他のデータで上書きされるまで実データ

部は残存しています。専門的な知識・技術をもってすれば、消去後であっても実データを復元させることも可能です。
シャープのデータセキュリティキットでは、ジョブデータやドキュメントファイリングデータの消去には、実データ部を乱数値等により上書きした後に、データの所在を示す情報を消去する方法を採っており、実データ部を復元できないようにします。

特長

■操作性の良さ
シャープのデータセキュリティキットによるデータの暗号化 / 実データ部の消去は、利用者が意識することなく自動的に機能します。そのため、機密データを扱う際に特別な操作を行うことなく、高いセキュリティレベルを維持できます。

ネットワークからの不正アクセスによる情報漏洩

● 脅威

例えば、多くのオフィスでは、インターネットへの接続に際してファイアウォールを設置するなど不正アクセス対策を施していると思います。しかし、イントラネット内部からのデジタル複合機への不正アクセスについては特に対策していないという場合が多いのではないでしょうか？重要なデータを入力したり出力したりするデジタル複合機は情報漏洩の格好のターゲットとなり得ます。

● 対策

ネットワークアドレス（IP/MAC アドレス）のフィルタリング
ネットワークインタフェースでは、特定の IP アドレスや MAC(マック) アドレス ※ をアクセス許可 / 拒否に指定することにより、複合機にアクセス可能なアドレス範囲を特定することで、不正なアクセスを防止します。
例えば、IP アドレスフィルタリングでは、社内ネットワークで特定の部署・グループの PC や端末のみでデジタル複合機を使えるように設定することができます。また、MAC アドレスフィルタリングでは登録していない端末 (外部から持ち込み社内ネットワークに接続した PC や端末等) をデジタル複合機に接続できなくすることができます。

※MAC アドレスによるフィルタリングは、アクセスを許可するアドレスの指定のみ可能です。

ネットワークポートの有効 / 無効設定 / ポート番号の変更
ネットワークプロトコルを用いて通信を行う際に必要なネットワークポートの有効 / 無効の設定や、ポート番号の変更を行なうことにより、ポートスキャン等、悪意を持ったアクセスを受け付けないようにしたり、外部への意図せぬデータ送信を制御したりすることが可能です。

特定発信元からの受信設定

ファクス、インターネットファクスの受信時に、不正な発信者からの送信により、通常の受信が阻害される、あるいは有害 / 不要な情報を受信することを防ぐために、特定番号 / 特定アドレスからの受信を拒否することができます。また、特定番号 / 特定アドレスからのみ受信することもできます。
番号 / アドレスの指定は、ファクス、インターネットファクスのそれぞれについて 50 件ずつ設定可能です。

IEEE802.1X

IEEE802.1X は、無線 LAN や有線 LAN にネットワーク機器を接続する際に、許可された利用者のみ接続を許可するための認証技術です。悪意を持つ者がネットワークに機器を接続し、デジタル複合機を不正使用するのを防ぐことが可能になります。認証プロトコルは EAP-TLS と PEAP に対応しています。

ドキュメントファイリングのパスワード保護

ドキュメントファイリングとは、再利用を前提としてデジタル複合機にジョブデータを保存する機能ですから、利用者の消去指示があるまでデータはドキュメントファイリングデータとしてデジタル複合機内に存在します。このドキュメントファイリングデータは、データ毎にパスワードを付加できるようになっています。このパスワードが一致しなければ、ドキュメントファイリングデータを再利用できないようにします。

ファクス回線からネットワークへの侵入について

当社デジタル複合機に搭載のファクスモデムソフトウェアは、スーパー G3/G3 通信をサポートするものです。PPP、TCP/IP フレームの送受信等の、電話回線を通じてコンピューターをネットワークに接続するためのプロトコルは実装しておらず、当社デジタル複合機を利用したファクス回線経由のネットワークへの侵入は不可能です。

撤去・廃棄されたデジタル複合機のメモリ装置からの情報漏洩

● 脅威

リース期間が終了、あるいはご購入後に撤去されたり、廃棄されたりしたデジタル複合機についても、お客様の管理から離れた後に情報が漏洩する危険性があります。

● 対策

個人情報及び本体内データの初期化機能

デジタル複合機の撤去・廃棄に際し、本体内の以下の情報を上書き消去（初期化）することができます。

- 本機内のジョブデータ、および、ドキュメントファイリングデータ
- アドレス帳及び関連する個人情報
- 利用者情報
- 登録プログラム、ファクス / イメージ送信定型文、ジョブログ
- システム設定

※ 一部搭載されていない機種があります。

ネットワーク入出力データへの不正アクセスによる情報漏洩

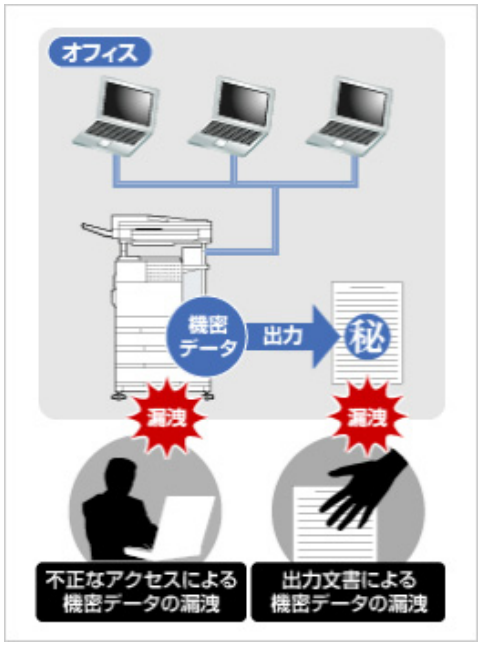
● 脅威

オフィスのネットワークでは、重要な情報がやり取りされています。これは、デジタル複合機のプリントデータやデジタル複合機のリモート管理等のネットワーク入出力データにおいても同様です。これらデジタル複合機のネットワーク入出力データが盗聴されることにより、情報が漏洩する可能性があります。

● 対策

SSL（Secure Socket Layer）暗号化通信

ネットワーク通信データの盗聴を防止するには、ネットワークプリントやWebブラウザーを介したデジタル複合機との通信は、ネットワーク通信データそのものを暗号化することが効果的です。これにより、たとえ盗聴されたとしても、その内容を解読することが非常に困難になります。



ネットワークを利用してパソコンからデジタル複合機へデータを送信するときや、パソコンの Web ブラウザーを利用してデジタル複合機の管理用Webページにアクセスするとき、E-mail、FTP サーバー等でのデータ通信には、SSL プロトコルを使うことにより、これらの機器間の通信を暗号化します。

暗号化PDFファイル対応(送信/ダイレクトプリント)

スキャンした文書をPDFファイル化する際に暗号化します。また、デジタル複合機のオペレーションパネルでパスワードを入力することにより、暗号化されたPDF ファイルの印刷も可能です。暗号化された PDF ファイルが通信途中で盗聴されたとしても、その内容を解読することは困難です。

IPsec

IP のパケット単位で暗号化を行なうことにより、通信途中でのデータ内容の盗聴や改ざんを防止します。

SNMPv3

デジタル複合機の管理に使用される通信も、暗号化をサポートする SNMPv3 により、盗聴を防止します。

誤送信による情報漏洩

● 脅威

イメージ送信とは、スキャンしたデータをファクス、E-mail、FTP などでオフィスや外部のファクス / サーバー / パソコンに送信する機能です。意図せず送信先を間違った場合、情報が漏洩する可能性があります。

● 対策

■宛先直接入力禁止
宛先指定にはアドレス帳を利用することにより、宛先の入力ミスによる誤送信を防止することができます。

■再送信キーの利用禁止
前の人が送信したアドレスに、誤送信してしまうのを防止します。

■宛先確認機能
宛先を一度入力した後、再度宛先を確認、もしくは、再度入力するダブルチェック機能で送信先の入力間違いを防止します。

■暗号化 PDF ファイル対応（送信）
送信ファイルに暗号化 PDF を指定することで、万一誤送信されたとしても、パスワードを知らなければ解読することができません。

■ FASEC 1 に準拠
FASEC とは、情報通信ネットワーク産業協会（CIAJ）がファクシミリ通信のセキュリティ向上を目指して制定したガイドラインの呼称です。
誤送信の防止や受信紙の放置防止など、ファクスデータにおいてもセキュリティ対策に努めております。

出力した紙文書の持ち去りによる文書データの漏洩

● 脅威

プリントやファクス出力を放置したままにしているのを見かけた方も多いのではないでしょうか。特にプリントの場合、忘れてしまっていることも多く、盗み見されたり、持ち去られたりして、情報漏洩して初めて気づくことになります。

● 対策

リテンション（親展プリント）機能

プリントデータをデジタル複合機に保存しておき、必要なときに本機の操作パネルからプリントする機能です。パソコンからプリントするときにパスワードを設定し、デジタル複合機に保存されているデータをプリントするときにパスワードを入力することにより、プリント結果を他人に見られたり持ち去られたりすることを防止します。

Sharp Print System によるプリントジョブの保護

複数のデジタル複合機を有している場合、デジタル複合機印刷運用システム「Sharp Print System」を使用することにより、「Sharp Print System」に対応した任意のデジタル複合機からプリントデータを出力することができます。印刷したいデジタル複合機が稼働中でプリントできない場合でも、他のデジタル複合機を利用することにより、本人がログインし印刷指示をすることでプリントが可能で、出力用紙の取り忘れや放置による情報漏洩を抑止します。

※Sharp Print System の詳細については、販売店にお尋ねください。

ファクス受信データホールド

ファクス受信データを出力せずに一旦メモリに保存します。あらかじめ登録したパスワードを入力することで出力します。ファクス受信データを出力する場合に比べ、盗み見や、用紙の持ち去りによる情報漏洩の危険を減らします。

不正コピーによる文書データの漏洩

● 脅威

オフィスで使用される機密文書には、「社外秘」「極秘」等と指定されていることが多いですが、悪意を持ってコピーされれば簡単に情報漏洩してしまいます。

● 対策

ドキュメントコントロール

機密文書の出力時に不正コピー防止データを埋め込むことができます。不正コピー防止データが埋め込まれた文書を、ドキュメントコントロール機能を搭載したシャープデジタル複合機で不正にコピーしようとした場合は、白紙出力やコピーキャンセルなどによって不正コピーを防止します。

※ オプションのデータセキュリティキットが必要です。一部対応していない機種があります。

権限の無いユーザーの使用による可用性の低下やデータの漏洩

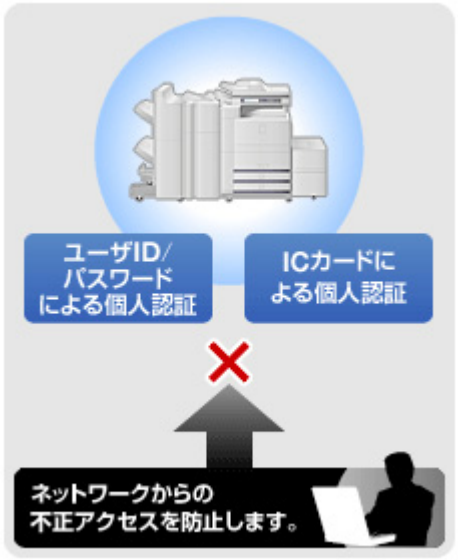
● 脅威

情報漏洩事件は、その多くが内部犯行であるという報告があります。内部の人間は必然的に機密情報に触れる機会が多く、故意ではなくとも、情報漏洩を起こす可能性がないとは言い切れません。また、使用権限の無いユーザーがデジタル複合機を使用する、また使用権限があってもその範囲を超えて使用することにより、本当に使用したいユーザーが使用できなくなったり、そのため作業効率が低下したりする恐れがあります。

● 対策

ユーザー認証 / 操作権限設定

ユーザー ID/ パスワード、または、IC カードによる個人認証により、デジタル複合機への不正アクセスを防止します。



■操作パネル /IC カードによる認証

ユーザー ID とパスワードの操作パネルからの入力、または IC カードによる個人認証 ※ を行うことで、許可された利用者のみ、デジタル複合機を使用可能になります。また、本体での認証とともに外部サーバーでの認証も可能です。

※ オプションの IC カードリーダーライターと IC カードが必要です。IC カードリーダーライターの詳しい内容につきましては、デジタル複合機をお買い上げの販売店にお尋ねください。

■操作権限の設定

ユーザーグループごとに、デジタル複合機の各機能の使用許可 / 禁止、また、デジタル複合機の設定を行う権限を付与することができます。

SharpAccountant Professional によるユーザー管理

デジタル複合機運用集中管理システム「SharpAccountant Professional」を使用することにより、複数のデジタル複合機をお持ちのオフィスでのユーザー認証や操作権限の管理を一元化することができます。また、各ユーザーの使用状況も集計することができ、オフィスに分散して設置されているデジタル複合機の効率的な運用をサポートします。

※SharpAccountant Professional の詳細については、販売店にお尋ねください。

使用状況の把握、および情報漏洩の心理的な抑止対策

デジタル複合機から情報漏洩を防ぐには、常にデジタル複合機の使用状況を把握しておくことが必要です。また、使用状況を把握していることを周知させることにより、情報漏洩に対する心理的な抑止対策効果が期待できます。

● 対策

ジョブログ管理機能により、誰がいつ何の作業を行なったか、どこへ送信したのかが把握できます。
デジタル複合機本体には、完了したジョブの履歴を最大６万件まで保存することができます。また、保存されたログは、外部のパソコンに取り出して一覧することができます。

5 機種別搭載セキュリティ機能一覧表

表の見方：
○ ····· 標準で対応しているセキュリティ機能です。
△ ····· オプションで対応しているセキュリティ機能です。
× ····· 対応しておりません。
－ ····· 該当機種では脅威として想定されません。
ネットワーク接続、暗号化 PDF ファイルのダイレクトプリント、およびイメージ送信にはオプションの装着が必要となる機種があります。

カラー複合機

脅威	対策機能	MX-2700G	MX-2310F MX-3111F MX-3611F	MX-2514FN MX-3114FN MX-3614FN MX-4140FN MX-4141FN MX-5140FN MX-5141FN MX-6540FN	MX-2640FN MX-3140FN MX-3640FN	MX-6201N MX-7001N
本体メモリ装置の持ち出しによる情報漏洩	保存されたデータの暗号化	△	△	○	○	△
	ジョブ完了後の実データ消去	△	△	○	○	△
	全データ消去	△	△	△	△	△
	データセキュリティキットのコモンクライテリア (CC) 認証	○	×	×	評価中	○
ネットワークからの不正アクセスによる情報漏洩	ネットワークアドレス（IP/MAC アドレス）のフィルタリング	○	○	○	○	○
	ネットワークポートの有効 / 無効設定 / ポート番号の変更	○	○	○	○	○
	特定発信元からの受信拒否設定	○	○	○	○	○
	IEEE 802.1X	×	○	○	○	×
	ドキュメントファイリングのパスワード保護	○	○	○	○	○
撤去・廃棄された複合機のメモリ装置からの情報漏洩	個人情報及び本体内データの初期化機能	×	○	○	○	×
ネットワーク入出力データへの不正アクセスによる情報漏洩	SSL（Secure Socket Layer）暗号化通信	○	○	○	○	○
	暗号化 PDF ファイル対応（送信 / ダイレクトプリント）	○	○	○	○	○
	IPsec	×	○	○	○	×
	SNMPv3	○	○	○	○	○
誤送信による情報漏洩	送信者名の選択禁止	○	○	○	○	○
	宛先直接入力禁止	○	○	○	○	○
	再送信キーの利用禁止	○	○	○	○	○
	宛先確認	○	○	○	○	○
	FASEC 1 準拠	×	○	○	○	×

脅威	対策機能	MX-2700G	MX-2310F MX-3111F MX-3611F	MX-2514FN MX-3114FN MX-3614FN MX-4140FN MX-4141FN MX-5140FN MX-5141FN MX-6540FN	MX-2640FN MX-3140FN MX-3640FN	MX-6201N MX-7001N
出力した紙文書の持ち去りによる文書データの漏洩	リテンション（親展プリント）	○	○	○	○	○
	Sharp Print System	×	△	△	△	×
	ファクス受信データホールド	○	○	○	○	○
不正コピーによる文書データの漏洩	ドキュメントコントロール	△	△	△	△	△
権限の無いユーザーの使用による可用性の低下やデータの漏洩	ユーザー認証 / 操作権限設定	○	○	○	○	○
	SharpAccountant Professional	×	△	△	△	×
使用状況の把握、および情報漏洩の心理的な抑止対策	ジョブログ管理	○	○	○	○	○

モノクロ複合機

脅威	対策機能	AR-N182FG	MX-M264FP MX-M314FP MX-M354FP	MX-M365FN MX-M465FN MX-M565FN	MX-M503N MX-M623 MX-M753	MX-M904 MX-M1054 MX-M1204
本体メモリ装置の持ち出しによる情報漏洩	保存されたデータの暗号化	—	○	○	△	○
	ジョブ完了後の実データ消去	—	○	○	△	○
	全データ消去	—	△	△	△	△
	データセキュリティキットのコモンクライテリア (CC) 認証	—	○	×	○	×
ネットワークからの不正アクセスによる情報漏洩	ネットワークアドレス（IP/MAC アドレス）のフィルタリング	○	○	○	○	○
	ネットワークポートの有効 / 無効設定 / ポート番号の変更	○	○	○	○	○
	特定発信元からの受信拒否設定	○	○	○	○	○
	IEEE 802.1X	×	○	○	○	○
	ドキュメントファイリングのパスワード保護	—	○	○	○	○
撤去・廃棄された複合機のメモリ装置からの情報漏洩	個人情報及び本体内データの初期化機能	×	○	○	×	○
ネットワーク入出力データへの不正アクセスによる情報漏洩	SSL（Secure Socket Layer）暗号化通信	○	○	○	○	○
	暗号化 PDF ファイル対応（送信 / ダイレクトプリント）	×	○	○	○	○
	IPsec	×	○	○	○	○
	SNMPv3	×	○	○	○	○
誤送信による情報漏洩	送信者名の選択禁止	×	○	○	○	○
	宛先直接入力禁止	○	○	○	○	○
	再送信キーの利用禁止	×	○	○	○	○
	宛先確認	×	○	○	○	○
	FASEC 1 準拠	×	×	○	×	○
出力した紙文書の持ち去りによる文書データの漏洩	リテンション（親展プリント）	×	○	○	○	○
	Sharp Print System	×	△	×	△	△
	ファクス受信データホールド	○	○	○	○	○
不正コピーによる文書データの漏洩	ドキュメントコントロール	×	△※1	△	△	△
権限の無いユーザーの使用による可用性の低下やデータの漏洩	ユーザー認証 / 操作権限設定	○※2	○	○	○	○
	SharpAccountant Professional	×	△	×	△	△
使用状況の把握、および情報漏洩の心理的な抑止対策	ジョブログ管理	×	○	○	○	○

※1 ドキュメントコントロール検知によるジョブ停止のみ対応しています。
※2 ユーザー認証は部門番号により行います。操作権限設定は非対応です。

A4 複合機・プリンター

脅威	対策機能	AR-N202FP	MX-C312 MX-C312SC MX-B382	MX-B382SC	MX-C300W	MX-C380P DX-C310P MX-B382P
本体メモリ装置の持ち出しによる情報漏洩	保存されたデータの暗号化	—	△	△	—	△
	ジョブ完了後の実データ消去	—	△	△	—	△
	全データ消去	—	△	△	—	△
	データセキュリティキットのコモンクライテリア (CC) 認証	—	×	×	—	×
ネットワークからの不正アクセスによる情報漏洩	ネットワークアドレス（IP/MAC アドレス）のフィルタリング	○	○	○	○	○
	ネットワークポートの有効 / 無効設定 / ポート番号の変更	○	○	○	○	○
	特定発信元からの受信拒否設定	○	○	○	○	—
	IEEE 802.1X	×	○	○	×	○
	ドキュメントファイリングのパスワード保護	—	○	○	—	—
撤去・廃棄された複合機のメモリ装置からの情報漏洩	個人情報及び本体内データの初期化機能	×	×	×	○	×
ネットワーク入出力データへの不正アクセスによる情報漏洩	SSL（Secure Socket Layer）暗号化通信	×	○	○	×	○
	暗号化 PDF ファイル対応（送信 / ダイレクトプリント）	×	○※1	○※1	×	○※2
	IPsec	×	○	○	○	○
	SNMPv3	×	○	○	×	○
誤送信による情報漏洩	送信者名の選択禁止	×	○	○	×	—
	宛先直接入力禁止	×	○	○	×	—
	再送信キーの利用禁止	×	○	○	×	—
	宛先確認	×	○	○	○	—
	FASEC 1 準拠	×	×	×	○	—
出力した紙文書の持ち去りによる文書データの漏洩	リテンション（親展プリント）	×	○	○	○	○
	Sharp Print System	×	△	×	×	×
	ファクス受信データホールド	×	○	○	○	—
不正コピーによる文書データの漏洩	ドキュメントコントロール	×	△	△	×	△※3
権限の無いユーザーの使用による可用性の低下やデータの漏洩	ユーザー認証 / 操作権限設定	○※4	○	○	○	○
	SharpAccountant Professional	×	△	×	×	×
使用状況の把握、および情報漏洩の心理的な抑止対策	ジョブログ管理	×	○	○	×	○

※1 送信のみ対応しています。
※2 ダイレクトプリントのみ対応しています。
※3 印刷のみ対応しています。
※4 管理者認証のみ対応しています。

問い合わせ先

お取扱い・お手入れのご相談は、お買いあげの販売店へお申し出ください。
販売店へご相談できない場合は、下記窓口に連絡下さい。
（沖縄地区を除く）

ナビダイヤル
0570 - 051001

受付時間 ●月曜～土曜：9:00～17:40
（日曜、祝日など弊社休日は休ませていただきます）

■IP電話・PHSからは･･･

東日本地区	043-332-9910
西日本地区	06-6794-2909

※ 当ナビダイヤルは、全国一律 10 円 / 分となります。なお、携帯電話・自動車電話からおかけの場合は、全国一律 10 円 /20 秒となります。
（ナビダイヤルは、NTT コミュニケーションズ株式会社のサービスです。）

※ ナビダイヤルをご利用になれない IP 電話・PHS からおかけの場合は、上表右の一般電話におかけください。

沖縄地区については、沖縄シャープ電機株式会社にお問い合わせください。
那覇サービスセンター　　098-861-0866
＜受付時間＞
月曜～金曜：9：00 ～ 17：40
（※ 日曜・祝日など弊社休日を除きます）

シャープ株式会社

シャープホームページ　http://www.sharp.co.jp/

製品の改良のために予告なくデザイン・仕様の変更を行うことがあります。記載の内容は 2013 年 12 月現在のものです。